NOKIA

Nokia 7705 Service Aggregation Router

Security overview for power utilities

Application Note

NOKIA

Contents

NOKIA

Introduction

This paper describes the security functionality of the Nokia 7705 Service Aggregation Router (SAR). It can be used by power utilities to ascertain how the 7705 SAR platforms meet security requirements, such as North American Electric Reliability Corporation Critical Infrastructure Protection (NERC-CIP) compliance in the heavily regulated energy sector. It can also be incorporated into security best practices frameworks and operations.

Security is quickly becoming a top priority for all vertical markets in general. Mandated by regulators in some industries, it is now essential for network operations teams to incorporate strong security when deploying communications systems. It is the responsibility of the operations organizations to make sure their systems are secure from malicious behavior. They must protect both end users and any critical infrastructure (such as the utility power grid) from security breaches that may damage the infrastructure, possibly causing catastrophic outcomes.

The level of protection must reflect the level of exposure to potential threats. Companies must analyze their networks within their operational context and assess potential risks, weighing that against the cost of implementing specific security measures to mitigate the risks.

This paper provides an overview of major 7705 SAR security features. It also outline how to apply them to prevent malicious behavior in some specific situations. Nokia recommends companies review their network threats with security experts to apply the best level of security within the network while taking advantage of key security features of the Nokia products being deployed.

Network security frameworks and standards

A methodology-based approach to protecting critical infrastructure networks provides a systematic means of addressing security risks. A framework must first be established to understand and evaluate risks and exposure. Reliable 24x7 electricity delivery is one of the most basic critical infrastructure services, and the power utility sector is an example of an industry leader in defining security frameworks for its members.

In addition, power utilities are currently transforming how they operate and deliver electricity to customers. This includes adopting more advanced communications systems for optimizing services for end-customers. IP-based applications are also becoming ubiquitous, from technological initiatives such as substation automation to advanced metering infrastructures for smart grids, and security risks are rising due to the use of these applications.

A recent study commissioned by USA Today indicated that there is an attack (cyber or physical) on the US power grid every four days [8]. With the increasing threat of cyber attacks on IP-based network infrastructure, several international standards organizations — NERC, IEC and ITU-T — have created comprehensive network security frameworks.

NERC CIP Version 5

To provide guidance to power utilities on how to address vulnerabilities and stop such attacks, in late 2013, the Federal Energy Regulatory Commission (FERC), the independent government agency that regulates the interstate transmission of electricity in the US, approved Version 5 of the CIP Reliability Standards for the Bulk Electric Systems of North America [4]. CIPv5 covers all security aspects of cyber systems, such as communications networks and computers that would impact the reliable operation of the Bulk Electric System (BES), including generation plants and high-voltage substations. The CIP5 suite also covers procedures for technical personnel who use cyber systems, security training, and audit requirements.

A later section, "Applicability of the 7705 SAR Security Suite to NERC CIPv5," summarizes how 7705 SAR security features map to CIP operational-control security requirements.

IEC 62351

To protect power system control operation for power utilities, the IEC published IEC 62351, "Power Systems Management and Associated Information Exchange — Data and communications security." [6] Under IEC 62351 are eight international standards that cover general communications network security for the power industry. The series identifies four security requirements:

1. Confidentiality: Preventing unauthorized access to information
2. Integrity: Preventing the unauthorized modification or theft of information
3. Availability: Preventing denial of service (DoS) and ensuring authorized access to information
4. Non-repudiation or accountability: Preventing the denial of action that took place or the claims of an action that did not take place

ITU-T X.805

ITU-T Study Group 17 has examined network security for more than a decade. The approved ITU-T X.805 recommendation, "Security Architecture for Systems Providing End-to-End Communications," [7] describes security requirements in eight dimensions, as outlined in the next section.

Details of ITU-T X.805 Security Architecture

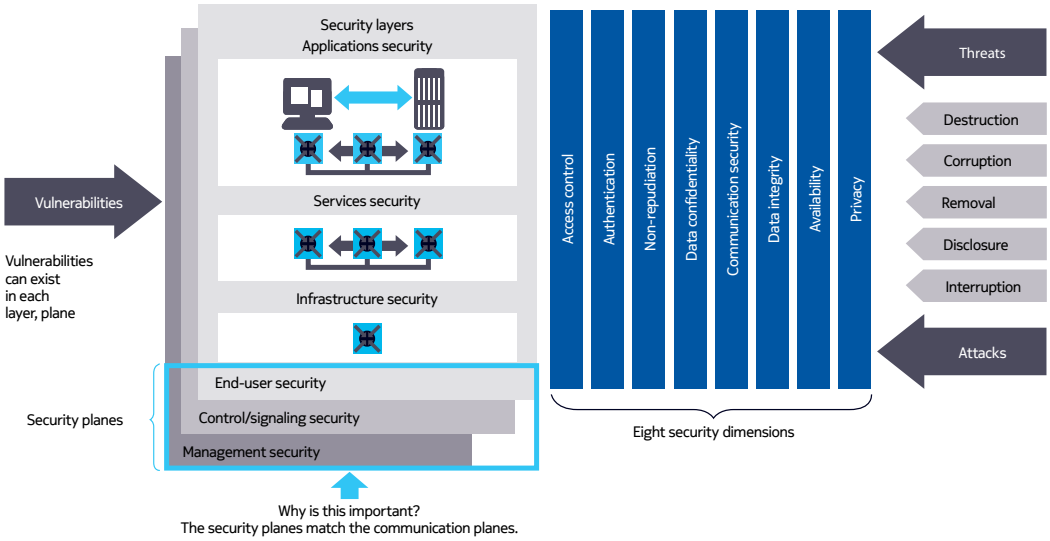
Nokia recommends applying a security framework to align different working groups within an organization and to promote common best practices. One such framework is established within the ITU-T organization. The ITU-T X.805 recommendation and the ISO 18028-2 standard are both based on the Nokia Bell Labs security model. It enables utilities to better implement governance programs that improve network security and eliminate potential threats. It also provides a systematic, comprehensive, multi-layered, end-to-end security framework to diagnose potential security threats in complex networks and ensure a consistent framework is used to apply network operations and management across the network.

Nokia has contributed heavily to this framework over the years. Therefore, this document uses the ITU-T X.805 security architecture as the baseline reference to bring structure to the analysis and discussion of how the 7705 SAR can apply security to the network. The remainder of this section is a summary of the ITU-T X.805 security architecture. Please read the ITU-T recommendation for more information.

The X.805 security architecture (Figure 1) provides a methodical, organized means of addressing threats to telecommunications networks and the type of actions to address these threats. The threats are identified in ITU-T Recommendation X.805 as follows:

- **Destruction** of information and/or other resources
- **Corruption** or modification of information
- **Removal**, **theft**, or **loss** of information and/or other resources
- **Disclosure** of information
- **Interruption** of services

Figure 1. ITU-T X.805 security architecture



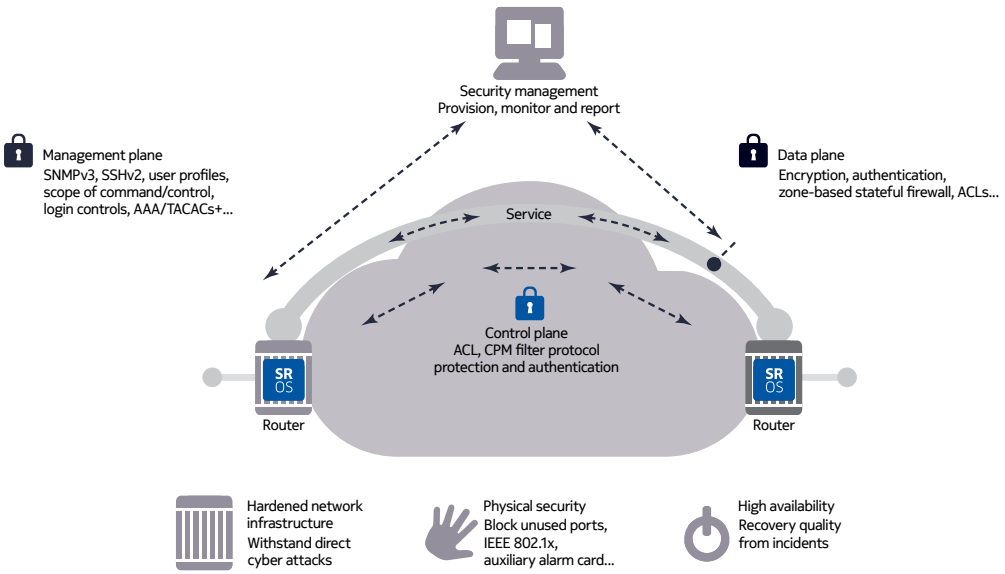
The architecture contains a total of 72 security perspectives — three layers used across three planes through eight dimensions — which can be used in all aspects and phases of a security program. The framework's three key security components are:

- **Security Dimensions** - a set of security measures designed to address a particular aspect of the network security. The Bell Labs model encompasses eight dimensions that protect against all major security threats. These dimensions are not limited to the network, but extend to applications and end-user information as well. In addition, the security dimensions apply to service providers or enterprises offering security services to their customers.
- **Security Layers** - a series of enablers for secure network solutions. The infrastructure layer enables the services layer, and the services layer enables the applications layer. The security architecture addresses the fact that each layer has different security vulnerabilities and provides the flexibility to counter the potential threats in a manner most suited to a particular security layer.
- **Security Planes** - a certain type of network activity protected by security dimensions. The security planes addressed in the Bell Labs model are the management plane, the control plane and the end-user plane. These security planes address specific security needs associated with the corresponding network management activities, network control or signaling activities, and end-user activities.

The above recommendation and standard can be applied in its entirety or on an as-needed basis to any or all aspects and phases of a successful security program, including:

- Definition and Planning - define comprehensive security policies, incident response and recovery plans, technology architectures and technical requirements
- Implementation - assess how security policies and procedures are rolled out and technology is deployed
- Maintenance and Health Check - manage and assess routine changes in architecture, network equipment, security policies and procedures, incident response and recovery plans

Figure 2. IP/MPLS security planes



7705 SAR security feature summary

The 7705 SAR is deployed to transport services for end-to-end communications using IP/MPLS as the principal transport infrastructure protocol. Therefore, the 7705 SAR must address both the infrastructure and service layers as described in the X.805 architecture.

The 7705 SAR helps utilities to build highly secure IP/MPLS-based communications networks for resilient and reliable delivery of critical operational and high-value business data. To address the eight ITU-T X.805 security dimensions, the 7705 SAR provides a comprehensive suite of security features for all management, control and data planes associated with the network infrastructure and virtual private network (VPN) services. Table 1 lists the 7705 SAR security features and functionality for the management, control and data planes in each ITU-T X.805 security layer.

Table 1. Summary of 7705 SAR security features in line with X.805 Security Framework

			Infrastructure Layer Security			Service Layer Security		
Security category	7705 SAR Implemented Functionalities	X.805 Security Dimension	MgMt Plane	Ctrl Plane	Data Plane	MgMt Plane	Ctrl Plane	Data Plane
Access Control List (ACL)	Data plane ACL (IP and Ethernet layer)	Access control	√	√	√	√	√	√
	Management ACL		√			√		
	Control Processor Module (CPM) filter ACL		√	√		√	√	
Firewall	Stateful zone-based configuration	Access control			√			√
	NAT				√			√
	Logging				√			√
Encryption	IPSec	Confidentiality, authentication and data integrity				√	√	√
	Network group encryption					√		√
Event Logging	Security log	Non-repudiation	√	√	√	√	√	√
	Change log		√	√		√	√	
Configuration security	Configuration authorization	Access control	√			√		
	Configuration change logging	Non-repudiation	√	√		√	√	
	Configuration backup	Availability	√	√		√	√	
	SNMPv3/SSH	Access control, authentication	√	√		√	√	

			Infrastructure Layer Security			Service Layer Security		
Security category	7705 SAR Implemented Functionalities	X.805 Security Dimension	MgMt Plane	Ctrl Plane	Data Plane	MgMt Plane	Ctrl Plane	Data Plane
Nodal availability	CPM filter	Availability	√	√		√	√	
	Dedicated management routing instance			√				
	Non Stop Routing (NSR)			√	√	√	√	
	Non Stop Forwarding (NSF)			√	√	√	√	
	Non Stop Signaling (NSS)			√				
	Graceful Re-start (Helper)			√	√		√	
Network availablity	Routing protocol authentication	Availability		√			√	
	Equal-cost multipath (ECMP)		√	√	√	√	√	√
	Fast Re-Route (FRR)			√	√		√	√
	Bidirectional Forwarding Detection (BFD)			√	√		√	√
User authentication	Local	Access control	√					
	RADIUS		√					
	TACACS+		√					
User authorization	Local	Authentication	√					
	RADIUS		√					
	TACACS+		√					

			Infrastructure Layer Security			Service Layer Security		
Security category	7705 SAR Implemented Functionalities	X.805 Security Dimension	MgMt Plane	Ctrl Plane	Data Plane	MgMt Plane	Ctrl Plane	Data Plane
Other Security Features	MD5 authentication (OSPF, RSVP-TE, BGP4, IS-IS, RIP and LDP)	Communication security	√					
	Generalized TTL Security Mechanism (GTSM)/RFC 5082	Communication security	√	√			√	
	SSHv1 and SSHv2	Communication security	√					
	Login back off mechanism	Authentication	√			√		
	Strong password		√			√		
	MPLS L2 VPN technology	Communication security, privacy				√	√	√

Security modes of operation

DoS attack prevention with ACLs

ACLs are configured separately for the data plane, control plane and management plane.

Data plane ACL

Regardless whether the traffic is IPv4, IPv6 or simply Ethernet, data plane ACL is the first line of defense for the mission-critical network, 7705 node and attached endpoints. The ACL matching criteria is configured as a linked list of entries including source/destination IP addresses, source/destination port numbers, protocol numbers, IP options and fragmentation. The matching rules are programmed at the edge of 7705 SAR packet forwarding hardware, simply known as the data path, to permit or drop incoming packets. All received packets are sent to an ACL, which will examine each packet against the link list of entries configured. The first match will result in an action: forward, forward next-hop (policy-based routing), forwarding class classification (also known as multifield classification or MFC) and drop. Unlike firewall rules (firewall capability will be explained later in the paper), ACL rules are stateless, meaning that they do not monitor the state of an upper layer (for example, Transmission Control Protocol (TCP) or User Datagram Protocol (UDP)) connection to perform an action based on connection state. A good network security design should include ACLs to remove unwanted packets as early as possible — at the ingress edge of the data path to minimize unnecessary load required further down the data path.

In addition to the security application, ACLs can be used for advanced service capability such as policy-based routing (PBR) and MFC as mentioned above. PBR and MFC use the matching criteria of an ACL to forward packets to a specific next-hop or an internal forwarding class accordingly.

Besides the IP layer, the 7705 SAR also protects Layer 2 services like VPLS with MAC layer-based ACLs. For example, Layer 2 MAC filters can be applied to ensure only known MAC addresses are allowed on the ingress of a Layer 2-based connection. All other traffic will be dropped, preventing ARP poisoning.

CPM filters for control and management plane

The control and management planes are concerned primarily with the operation, administration, maintenance and provisioning (OAM&P) of individual network elements, such as the 7705 SAR. Securing access to the 7705 SAR's network control and management resources is the key to ensure proper network services and operations.

After the data plane ACL, another layer of ACL, known as the CPM filter, can also be used to limit who can send control and management traffic destined to the router. This will help to prevent DoS attacks and protect the router's control and management infrastructure from being manipulated and overwhelmed. Both IPv4 and IPv6 filters are supported.

IPv4 CPM filters can use the following information to allow or deny access to the control and management planes for:

- DiffServ Code Point (DSCP) name - matching DSCP names
- Destination IP address and mask - matching destination IP address and mask values
- Destination port/range - matching TCP or UDP values
- Fragmentation - matching fragmentation state of packets
- Internet Control Message Protocol (ICMP) code - matching ICMP code in the ICMP header
- ICMP type - matching ICMP type in the ICMP header
- IP option - matching option or range of options in the IP header
- Multiple IP options - matching state of multiple option fields in the IP header
- Option present - matching state of the option field in the IP header
- Source IP address and mask - matching source IP address and mask values address ranges are configured by specifying mask values, the 32-bit combination used to describe the address portion that refers to the subnet and the portion that refers to the host. The mask length is expressed as an integer.
- Source port/range - matching TCP or UDP port and range values
- TCP ACK - matching state of the ACK bit set in the control bits of the TCP header of an IP packet
- TCP SYN - matching state of the SYN bit set in the control bits of the TCP header of an IP packet

IPv6 CPM filters drop or accept incoming packets based on the following match criteria:

- DSCP name
- Destination IP address
- Destination port
- ICMP code
- ICMP type
- Source IP address
- Source port
- TCP ACK
- TCP SYN

Advanced endpoint protection with stateful zone-based firewall

The firewall is another vital line of defense to protect devices (also known as endpoints) attached to the network. A stateful, zone-based firewall is available on the following 7705 SAR platforms:

- SAR-18
- SAR-8
- SAR-H
- SAR-Hc
- SAR-W
- SAR-Wx
- SAR-X

The 7705 SAR natively implements the firewall in the data path instead of integrating a software-based firewall appliance, as in some other router platforms in the industry. This native approach ensures low latency, quality of service (QoS) and high throughput performance as required in mission-critical services and networks. In addition, the firewall is designed to work seamlessly with other security functionalities on the 7705 SAR such as encryption. It monitors communication sessions state and provides deeper packet inspection than ACLs to eliminate more advanced cyber security threats. The main firewall functionalities are the following:

1. Near-line-rate throughput and negligible incurred low latency
2. Stateful inspection of upper layer communications sessions including TCP, UDP, DNS and ICMP
3. Application (DNS and ICMP) awareness, strict TCP and application layer gateway (ALG) functionality awareness to safeguard against replay attack
4. Service awareness in virtual private routed network (VPRN) and global routing table (GRT) including firewall inspection between access and IPSec/MPLS tunnel network uplink in VPRN services
5. Per-entry and per-zone session number tracking

6. Extensive logging of all sessions (allowed and disallowed) with 5620 SAM and a Syslog server
7. Entry-based traffic rate policing
8. Ease of configuration via 5620 SAM policy global distribution infrastructure and zone-based approach
9. Flexible, policy-based network address port translation (NAPT) functions, including source NAT (SNAT) and destination NAT (DNAT)

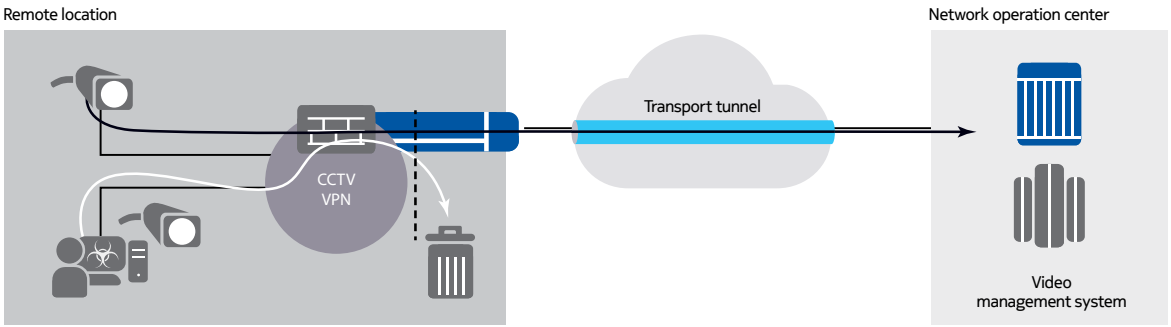
The listed firewall functionalities increase the security of the networks by doing deeper packet inspection and session tracking in addition to the ACLs.

Service-aware firewall

It is important to deploy firewalls in mission-critical networks to provide maximum security to industrial infrastructure operations. To provide basic service segregation and security, associated endpoints of different services are placed into different VPN services. As cyber attacks are becoming more persistent and sophisticated, a service-aware firewall becomes crucial to stop malicious traffic.

In Figure 3, an attacker compromises a surveillance camera. Because of firewall protection, illicit traffic sent by the hacker to reach other application endpoints or engage with the video management system (VMS) would be stopped. For example, efforts by the hacker to send a lot of traffic to the VMS will be rate-policed by the firewall, thwarting the DoS efforts.

Figure 3. Firewall stops cyber attack via a compromised device



Zone-based firewall

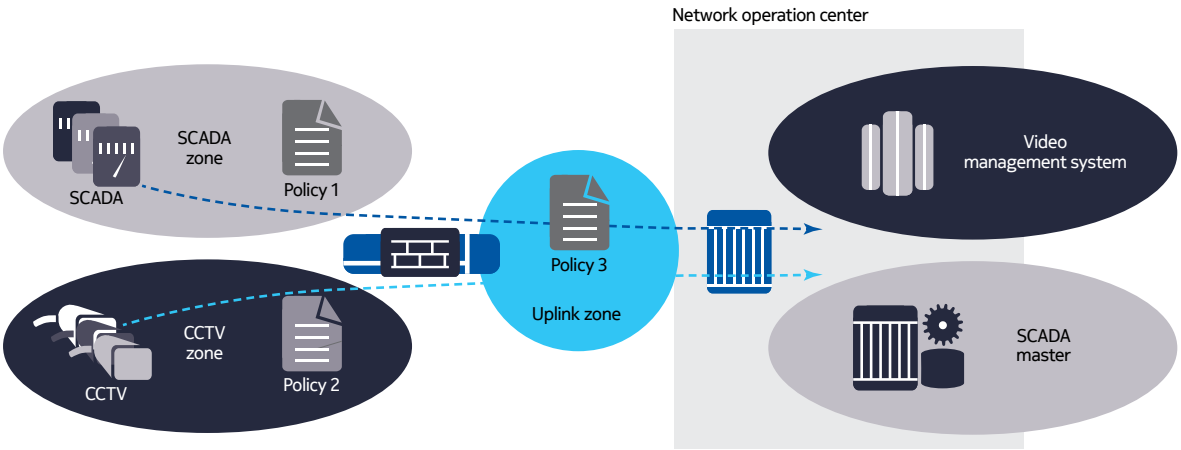
The firewall configuration approach is based on a zone-based design. It can be configured for VPRNs, internet Enhanced Service (IES) and just basic GRT. When used in a VPRN, in addition to regular Layer 3 interfaces, it can also be applied to transport tunnels including label switched path (LSP), encrypted LSP with network group encryption (NGE) and IPSec. All received VPRN traffic will be decrypted first if necessary, and inspected before being forwarded internally. Before the traffic is sent to the next hop router, it is inspected by the firewall, encrypted if necessary, and transmitted through LSP or IPSec tunnel.

Zone concept

A zone is a group of Layer 3 interfaces that have the same security needs. Zones can be applied to any Layer 3 services like VPRN or IES or under GRT. Zone configurations use a security policy that defines the rules to specify actions performed on packets. These actions can be forward, reject/drop or NAT.

Zones can be strategically positioned on access and/or network Layer 3 interfaces to give the operators the needed efficiency and flexibility to design security policy with firewall. For example, if the operator has a need for a single common security policy on the uplink to firewall any traffic entering from core network, a single zone can be configured and the uplink interface bound to this zone. On other hand if the operator has a need to have a more granular security policy for other interfaces, a different zone can be created with different security policy configured to cater for different security requirements. Figure 4 shows the above two concepts, with a single zone on the uplink and two access zones for IEDs such as SCADA remote terminal unit (RTU) and CCTV domains on the access IES or VPRN Layer 3 interfaces with different policy imposed.

Figure 4. Firewall zone concept



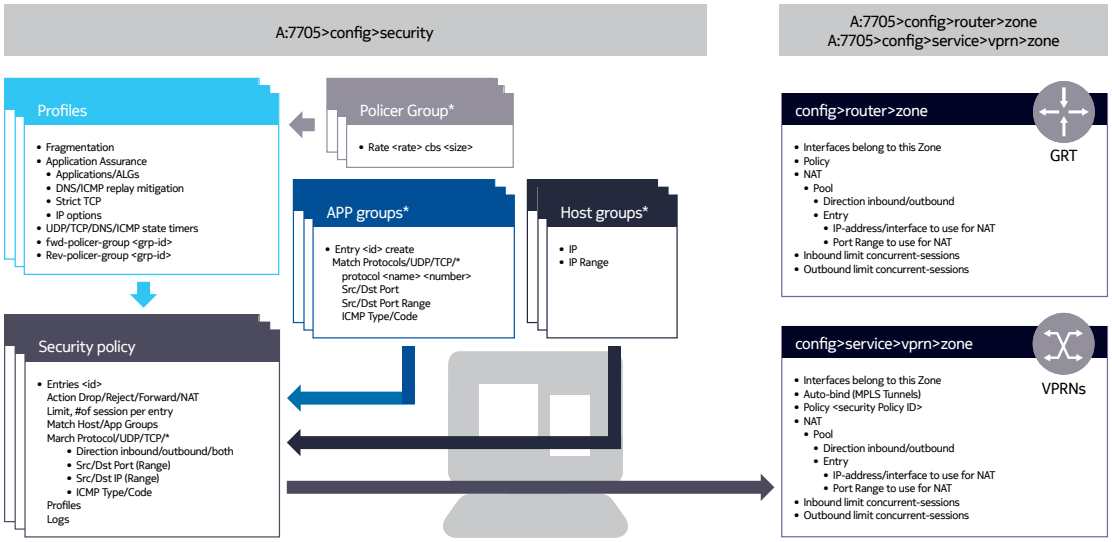
Security policy comprises a list of entries that contain matching rules to compare with incoming packets and a subsequent action if matched. If a packet matches the rule, the action will be carried out. Traditionally, policy can be created only via a linked list of entries. To enable efficient and flexible policy configuration, a group-based approach with applications group, host group, profile and policer group can be alternatively use.

Application group is a list of services associated with applications and consists of a combination of protocol type, source port, destination port, or ICMP type and code. Host group is a list of IP addresses or IP address ranges that are associated to hosts that may attempt to establish sessions through a particular zone. Both application groups and host groups can be reused and re-applied to multiple policies, thus allowing an efficient creation and elegant management even when there are long lists of policies and rules.

Profile defines the characteristics of allowed sessions. It includes: allow-IP-fragment, allow-IP-option, strict TCP check, and session timeout for cases such as icmp-query, tcp established, tcp-syn, tcp-time-wait, tcp-transitory, udp, udp-dns, udp-initial. Profile can also define application layer policies including ALGs and DNS/ICMP mitigation attack configurations. Policer group will be discussed later in the paper. Figure 5 shows the hierarchical relationships among profiles and groups.

Managing security policy for a sizable network is always a challenge. The 5620 SAM can manage security policy and its associated groups, profile centrally and distribute policies to 7705 SARs in the network.

Figure 5. Firewall policy and group hierarchy



The firewall supports NAPT as part of its policy configuration options, including SNAT and DNAT.

In summary, the various options, modular policy construction and zone-based design render extensive flexibility to operators when they are designing and implementing security measures to protect their mission-critical infrastructure.

High performance throughput and session management

Traditionally, enabling firewall on a router would degrade router performance significantly. However, with the 7705 SAR's unique network processor hardware capability, little performance degradation occurs, resulting in very high firewall throughput.

The 7705 SAR further optimizes throughputperformance by a policy scanning mechanism. Policy sets only once – when a session is being established. This policy scanning mechanism is performed on the CPM for the first few packets. After the packet is matched against a rule in the policy, the 7705 SAR performs the actions associated with the policies configured for the zone. If the action requires a session object be established for tracking (for example, forward, drop or NAT), the signature of the session objects are downloaded to the network processor and all subsequent packets for this signature are quickly processed. This allows the 7705 SAR to provide near-line-rate firewall performance with extremely low latency on those sessions. Packets are denied admission to the router if they are not associated with an established signature or do not pass the rules in the applied security policy. Sessions that require additional processing, such as strict TCP checking, will be always extracted to CPM.

Two policy actions will result in packets being denied admission: “action reject” and “action drop.” While both actions result in packets not admitted, they are optimized for different illicit traffic conditions. On one hand, if operators see there are only a few high-volume illicit sessions, “action drop” is ideal as the CPM will create and download to network processors a signature for each session, optimizing router performance. On the other hand, if there are many low-volume illicit sessions, “action reject” is more suitable as the CPM does not create a signature, saving CPM resources.

It should be noted that the 7705 firewall also supports a reject action. This action disallows the packet based on the matching rules on the CPM and does not create a signature to be downloaded to the network processor, unlike “action drop,” which downloads the signature to the network processor for subsequent dropping of the packets matching that signature. There is a fine line between deciding between “action reject” and “action drop.” If the user feels there is a high stream of packets with the same signature that needs to be dropped on the network processor without burdening the CPM, the “action drop” should be configured against the match. It should be noted that “action drop” will consume a firewall session. On other hand, if the user feels there could be random low-throughput packets that need to be discarded, “action reject” is more suitable to discard the packet on the CPM without creating a session and consuming session resources from the firewall.

Session tracking and policing

Session tracking

The firewall can track and cap the number of established sessions that matches an entry of a security policy and a security zone. In some cases, operators want to limit the number of sessions between a pair of IP hosts. For example, if there are only five CCTV cameras installed in the remote location, only five sessions should be established. If an attacker tries to launch a 6th session, trying to break out of the firewall, it will be stopped.

Session limit can also be configured in a hierarchical fashion to allow more flexibility. Using the same example above, the operator can allow a maximum number of five sessions in the policy and seven in the security zone that contains the policy, which is one layer above security policy. This allows the flexibility of allowing the total number of CCTV sessions and other application sessions to be seven, while the number of CCTV sessions remains five or under.

Traffic policing concept on 7705 SAR firewall

The firewall also includes unique traffic policing (also known as rate limiting) capabilities on a per-entry basis. To simplify configuration efforts, the policing rate is configured in a policer group. The rate can be forward, reverse or bidirectional and the group can be applied to each entry. This is an effective tool to protect in the case of a compromised endpoint; the attacker cannot send out more traffic than allowed, minimizing the damage incurred.

Application-aware firewall

The firewall has gone beyond traditional Layer 3 and Layer 4 inspection and has become application-aware. Coupled with deep inspection and protocol intelligence, it can be an application layer gateway (ALG) for applications such as FTP and TFTP, as well as stopping DNS and ICMP replay attacks. It can also ensure that the strict TCP flow control mechanism[1] is followed, securing a TCP connection.

1 RFC 793 Transmission Control Protocol https://datatracker.ietf.org/doc/rfc793/

ALG for FTP and TFTP

FTP/TFTP has a control channel and a data channel. The client communicates with the server via a well-known control channel (TCP port 21 for FTP and 69 for TFTP) and negotiates the data channel on another TCP port to be used for file transfer. As such the data channel TCP port has to be open to allow the data through. Since this port is typically assigned randomly, the operator usually needs to open a wide range of TCP ports to allow this data channel through, leaving the network susceptible to cyber security attacks.

An FTP ALG closes all unnecessary ports with the exception of the FTP control channel TCP port. The application-ware firewall will examine the control channel continuously to detect the FTP control channel, notes the data port negotiated between client and server, and will allow data through that port only for the duration of file transfer. It will close the port when the control channel indicates the file transfer is concluded, thus stopping cyber attacks via that port.

ICMP/DNS replay mitigation

Another common type of cyber attack is the use of the ICMP and DNS application layer protocols. (Usually for these protocols there is a request message (ICMP request and DNS request)). For each request there should be only one response. Attackers can continually reply this valid response back to the requester and overwhelm it. By tracking each received request's ID, the firewall allows only the first copy and disallows any additional responses that have the same ID.

Stateful firewall

Other common cyber attacks are DoS attacks like "SYN Flood" or "Half Open TCP" attack with TCP connection. The attacker overwhelms the server's memory and CPU resources by opening a TCP connection in a half-open state or "SYN" state so that it can no longer serve legitimate client requests. If the firewall does not detect that TCP state change occurs within a configured TCP timer, it will close the TCP connection.

The firewall can also monitor the state of UDP/DNS/ICMP connections. An appropriate timer can be assigned for each state of these connections, If it is in that particular state for more than the period dictated by the specific timer, the connection can be disconnected. In this way, the resources used by the servers in these types of attacks are minimized.

Data confidentiality, integrity and authenticity with encryption

There are two main modes of operation for encrypting and authenticating user data services:

1. IPSec
2. Network Group Encryption

The 7705 SAR platforms that support both these modes of encryption include:

- SAR-18
- SAR-8
- SAR-X
- SAR-H
- SAR-Hc
- SAR-W
- SAR-Wx

For the 7705 SAR-18 and SAR-8, encryption-capable adapter cards are required. These cards should be used for network-facing interfaces where encrypted traffic is expected to pass. The line cards that support encryption include:

LINE	SAR-8	SAR-18
8-port GE SFP Line Card (V3)	√	√
6-port 10GE Line Card	√	√
1-Port 10GE/10 Port 1GE Line Card (V2)		√

Encryption and authentication on the 7705 SAR platforms are supported by hardware accelerators built into the various 7705 SAR platforms and line cards mentioned above. These hardware accelerators allow the 7705 SAR to provide very high rates of encryption throughput that helps to ensure network links are used to their fullest wherever possible. In addition, 7705 SAR hardware acceleration incurs a negligible amount of latency as packets are being encrypted or decrypted.

IPSec encryption

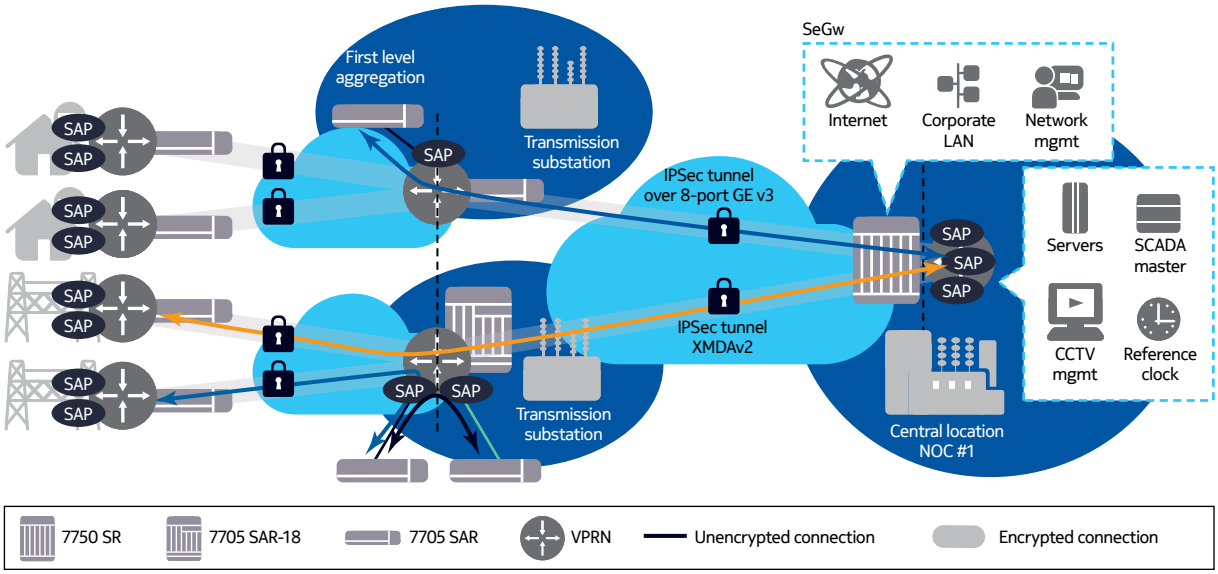
The 7705 SAR supports the creation and management of IPSec tunnels to encrypt and authenticate IP packets and flows. After the key establishment phase done by the internet Key Exchange (IKE) protocol, the IPSec tunnel is up and running without any need of signaling across the two tunnel endpoints. Therefore it is also called a light tunnel. This is in contrast to MPLS Layer 3 services, which use Multiprotocol BGP4 (MP-BGP4) to signal and advertise routes and labels between two provider edge routers. The MP-BGP4 session is transported outside the transport tunnel. With IPSec, all route advertisements like MP-BGP4 will be carried out over the IPSec tunnel. In this way, routing information will be encrypted.

Typically, IPSec tunnels are used to provide protected connectivity between two networks in the same VPN domain, in a spoke-to-spoke or hub-to-spoke topology, over portions of an IP backbone network where privacy is a concern or is untrusted. In the case of hub-to-spoke topology, to facilitate VPN route distribution, routes can be advertised via the IKE protocol and installed at hub side via a technique called reverse route injection (RRI). Alternatively, a customer routing protocol (for example, BGP4) can be run between their networks over the IPSec tunnel securely.

The 7705 SAR IPSec solution is interoperable with the Nokia 7750 Service Router (SR) integrated Service Adapter (ISA) application and the 7750 SR can provide the security gateway function for communications from central locations to remote sites where 7705 SARs may exist.

Figure 6 illustrates a typical application of the 7705 SAR IPSec tunnel functionality in a power utility network.

Figure 6. 7705 IPSec network application



The network topology in Figure 6 is hub-to-spoke. IPSec tunnels from access level 7705 SARs can be terminated at hub locations, such as SAR-8 or SAR-18 at transmission substations. These hub locations can then aggregate the traffic into a single IPSec tunnel that terminates on 7750 SR nodes at the central location. Routing decisions at the hub locations from access toward the central location are based on customer IP/Layer 3 information, either as part of the GRT or between VPRNs.

It should also be noted that IPSec can be used for spoke-to-spoke connectivity as well if necessary.

The types of encryption and authentication algorithms available on the 7705 SAR provide a high degree of security and privacy. IPSec authentication algorithms include MD5, SHA-1, SHA-256, SHA-384, SHA-512 or null. IPSec encryption algorithms include 3DES, AES-128, AES-192, AES-256 or null.

It should be noted that currently the 7705 SAR supports a pre-shared key to established IKE between two nodes. As stated in 7.0 R6, the IKE phase one can be established via public key infrastructure (PKI) and x.509 certificates.

PKI enables key management and generation by vendors and authorization of these keys by some centralized authority like federal governments and/or the utilities themselves.

Network Group Encryption[2]

Network group encryption (NGE) enables user data traffic and services riding over MPLS to be encrypted end-to-end (Figure 7). It does so without needing to establish and manage meshes of IPSec tunnels between nodes or convert all traffic to IP routed packets, as is required with encryption techniques such as IPSec. It is often cumbersome or problematic to convert Layer 1 TDM services — such as serial data links, T1/E1 circuits, IEEE C37.94 interface, FXO/FXS or E&M connections, or other Layer 2 services – such as virtual leased line (VLL) of different types and multipoint VPLS, as well as Layer 3 VPRN services, before encrypting.

Figure 7. NGE service level encryption

NGE is a simple and efficient way of providing an encryption privacy option for services over MPLS that do not intrude on the underlying services riding over MPLS. NGE is not limited to Layer 3 services as in IPSec; it can also provide encryption for Layer 1 and Layer 2 services that use MPLS as the main transport mechanism. In summary, NGE can provide group-based encryption to Layer 1 TDM, VLLs, VPRN, IES and even Layer 2 VPLS-based services in a group-based manner.

NGE provides two main modes of operation.

1. Service Distribution Point (SDP) encryption - MPLS user plane traffic that uses SDPs for transport can be encrypted by simply enabling encryption on SDPs. Types of traffic include VPRN or IES services that use spoke SDPs, VPLS using spoke or mesh SDPs, Ethernet pseudowires (Epipes) and constant-bit-rate TDM pseudowires (Cpipes).
2. VPRN encryption - any VPRN traffic that uses MP-BGP as the routing function is available for NGE.

Enabling NGE for services is simplified by minimizing the configuration tasks required. For SDP encryption, simply “turn on” encryption for the SDP and all traffic that uses the SDP is encrypted. For VPRN encryption, simply “turn on” encryption for the VPRN and all traffic for that VPRN is encrypted.

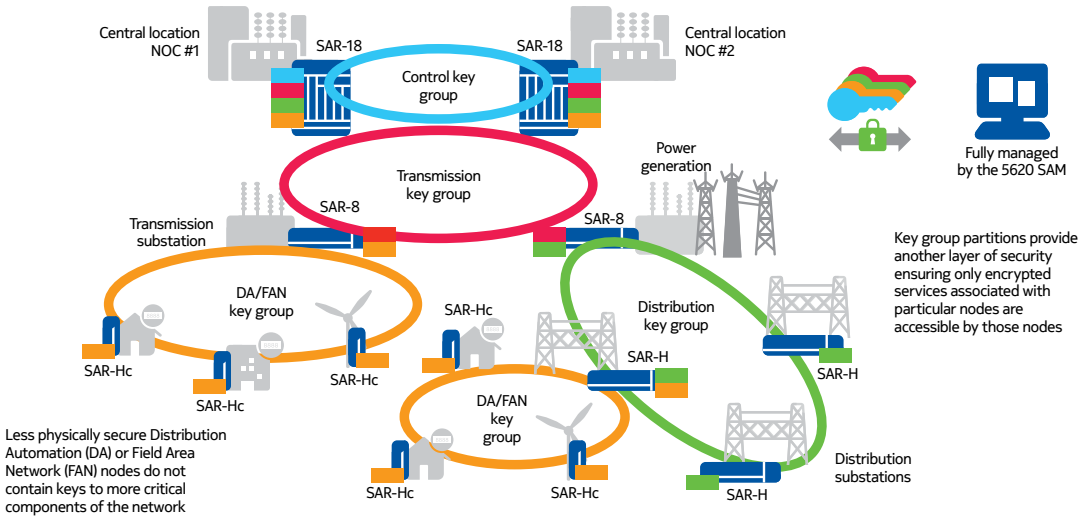
NGE provides a tiered approach to managing keys in the network. This is accomplished using key groups and configuring SDPs or VPRNs to use a specific key group depending on the security policies for the services using the SDP or VPRN. For example, in a power utility smart grid network, there may be different levels of criticality that need to be considered. The distribution automation network (DAN)/field area network (FAN) may be considered less critical than transmission or distribution substation network equipment. Due to the differences in criticality of infrastructure, ensuring nodes at risk do not contain more critical information than is necessary is ideal.

2 For more detailed information on NGE, please read “Seamless Encryption for Mission-Critical Networks” http://reources.alcatel-lucent.com/asset/187584

Encryption keys for sensitive portions of the network should not be available where nodes are at risk. The 7705 SAR NGE feature allows operators to partition encryption keys between different security domains in a network (Figure 8). For example, if an attacker attempts to gain access to the network from a DA/FAN location — where added physical security measures may be impractical or cost-prohibitive and therefore more prone to attack — the attacker will not be able to gain sensitive key information for other parts of the network. The attacker would be limited in scope by any attempted attack with key group domains and partitioning in place.

Figure 8 illustrates an application of NGE key group partitioning.

Figure 8. Encryption partitioning with key groups



NGE is tightly integrated with the Nokia 5620 Service Aware Manager (SAM) for key group management associated with MPLS services that are configured on nodes. The 5620 SAM acts as the key manager for all nodes and provides the relevant keys in key groups used to perform encryption and authentication. The 5620 SAM ensures that all nodes in a key group are synchronized and that only those key groups relevant to a particular node are downloaded with sensitive keys.

The 5620 SAM also re-keys a key group with zero outage time during a re-key procedure. Different key groups can be rekeyed at different times, if desirable, or all can be re-keyed network-wide simultaneously. The NGE feature using the 5620 SAM as a key manager was designed to maximize network uptime in the event of a network failure (for example, from a natural disaster). Security functions in the network and critical network traffic are maintained during events such as nodal reboots due to power failure, or nodes coming back on-line due to link restoration.

Advantages of the 7705 SAR NGE solution include:

- MPLS-based encryption of services that includes all types of Layer 1, Layer 2 and Layer 3 traffic, without needing to convert to IP before encryption
- Full MPLS operations benefits, including restoration techniques (e.g., FRR, and primary/backup LSPs), area border router (ABR)/autonomous system border router (ASBR) function, traffic engineering and OAM functions
- High scalability, since scale of encrypted services over MPLS is now tied to the scalability of the MPLS network itself
- Powerful security domain partitioning of a network and services using key groups
- Hitless, network-wide rekeying procedures of key groups using the 5620 SAM
- High availability and recovery of security functions for critical data traffic in the event of network outages or failures

Authorization, authentication and accounting

User profiles, authentication, IEEE 802.1x – Extensible Authentication Protocol

User profiles

Profiles can be configured to deny or permit access to a hierarchical branch or specific commands. Profiles are referenced in a user configuration. A maximum of 16 user profiles can be defined. A user can participate in up to 16 profiles. Depending on the authentication requirements, passwords are configured locally or on a RADIUS or TACACS+ server. User privilege can also specify which protocols, such as Telnet, SNMP, SCP, FTP, or console access are allowed by a user to access the system.

User authentication

The 7705 SAR software supports three methods of user authentication:

1. Local password authentication
2. Remote Authentication Dial-In User Service (RADIUS)
3. Terminal Access Controller Access Control System Plus (TACACS+)

Full support for RADIUS and TACACS+ secure access methods are supported from an access, authentication, and accounting (AAA) standpoint. Using RADIUS or TACACS+ to manage user authentication and authorization is recommended over using the local database included in 7705 SAR nodes. A utility should decide on the various user types and the required access for each. Specific users should have access to areas of the network elements that allow them to do their work, but have restricted access to configuration items that could affect network operations or security.

The 7705 SAR can be configured with up to five different server addresses along with the relative priority of the servers so network events do not prevent a user from gaining access to the platform.

IEEE 802.1x, Extensible Authentication Protocol (EAP)

IEEE 802.1x or EAP is supported on the Ethernet ports to enhance security in environments such as substations, where security requirements are increasingly important. 802.1x queries are converted to RADIUS requests to centralize authentication on an AAA server.

By default, all non-configured ports are disabled on the 7705 SAR, which restricts access to the network.

Security logging and access

The 7705 SAR can log security-related events on the main system log or on a separate security log. The two primary logging events that should be monitored are Security Events and Change Events:

- Security Events - The security event source is all events that affect attempts to breach system security, such as failed login attempts, attempts to access MIB tables to which the user is not granted access, or attempts to enter a branch of the CLI to which access has not been granted.
- Change Events - The change activity event source is all events that directly affect the configuration or operation of the node.

The 7705 SAR generates events that notify the operator of attempts to breach system security, such as failed login attempts, unauthorized attempts to access MIB tables or to enter a branch of the CLI to which access has not been granted. Failed attempts to authorize routing protocol exchanges also generate an event. Operator-defined logging policies determine if and how the event is presented to the operator (that is, does the event result in a log and to which type of log is the event sent; for example, Console, Syslog or file.

If the 7705 SAR management plane is engaged in a dictionary attack, the system provides an exponential back-off mechanism for the console port and will terminate SSH and Telnet sessions after four failed login attempts.

Configuration command logging

All operator actions that affect the configuration or operation of the node also generate an event. As with security logging, operator-defined logging policies determine if and how the event is presented to the operator.

Node management access

The 7705 SAR fully supports SSH version 1 and 2, Secure Copy (SCP), Secure FTP (SFTP) and IPSec. These protocols are disabled by default and need to be enabled to be used.

The 7705 SAR also has management traffic queues that allow the user to separate traffic based on priority and application to protect the control plane against malicious attacks. All network management configuration activities should use SNMPv3 with security enabled to prevent unauthorized users from accessing information transmitted between the network element and the network managers. Users connecting directly to the network elements for CLI configuration should use SSHv2. SSHv2 uses an enhanced networking implementation and is considered more secure and efficient than SSHv1.

For authentication and authorization purposes, the provider should start by changing the default login of the network element. This will help to prevent users from accessing the platform with basic password retry attempts. It will also help to prevent access by using the console port if physical network element access is not secured (for example, customer premises equipment is not in a locked cabinet).

NOKIA

Threat mitigation tactics

As explained above, the Nokia 7705 SAR has a full suite of security features. Many of these features can be used in security best practices to meet security requirements. While not all inclusive, Table 2 represents an excellent cross-section of features to consider while implementing a sound and robust security framework to mitigate some common threats.

Table 2. Example node security threat mitigations

Security Threat	Miti4gation	Comment
Spoofing IP addresses	Stateful firewall	Using a stateful firewall and ACL features can limit the data flow between known entities within the network on a per-service access point or network interface basis
	ACLs	
	Authentication	
Sniffing passworks	SNMPv3 security	SNMPv3 security helps limit the risk by providing confidentiality and integrity features
	Secure Shell (SSH)	Use SSH to provide encryption of passwords and configurations
Session hijacking	Stateful firewall and ACLs	Use stateful firewall and ACL features to limit where and to whom traffic can flow
	Authentication	Use authentication protocols such as HMAC-MD5 to protect against protocol session hijacking
	IPSec	Use IPSec to provide encryption of the sessions
AAA attacks	SNMPv3 security and SSH	Use hashing and encryption to help prevent access to the network device
	Exponential back-off	Help to prevent against dictionary attacks
	CPM and management access filters	Restrict access to the device by creating an ACL specifically for the CPM via the backplane or the management port.
DoS attacks	Stateful firewall, ACLs, CPM filters	Stateful firewall, ACLs, or CPM filters can be configured to reject SYN messages for users with IP addresses outside the closed user group.

Security Threat	Miti4gation	Comment
Physical security	Disable all unused Ethernet ports on the system	The 7705 SAR uses the concept of service access point (SAP) and other service associations. Without initial configuration of the port there is no access to the system and the network.
	802.1x authentication	802.1x authentication can be used to make sure attached Ethernet hosts or devices are authenticated before they are allowed to pass traffic.
	Strong management port password configuration	The management port and console port require password authentication. It is recommended that the default be changed prior to or during initial configuration and commissioning.

Applicability of 7705 SAR security to NERC CIP Version 5

The NERC Version 5 CIP Cyber Security Standards is a suite of CIP standards (CIP-002-5.1, CIP-003-6, CIP-004-6, CIP-005-5, CIP-006-6, CIP-007-6, CIP-008-5, CIP-009-5, CIP-010-2 and CIP-011-2). CIP-002-5.1 requires the initial identification and categorization of Bulk Electricity System (BES) cyber systems, and the rest of the standards require a minimum level of organizational, operational and procedural controls to mitigate risks to BES cyber systems.

Power utilities must dedicate resources to design and execute plans to fulfill organizational and operational controls, and the 7705 SAR can help implement procedural controls. Table 3 summarizes the applicability of the 7705 SAR security features to CIP operational-control security requirements.

Table 3. NERC CIPv5 mapping to 7705 SAR

7705 SAR Security Features	7705 SAR Implemented Functionalities	Applicability to CIP Requirements
Services security	NAT	CIP-003-6 R2 CIP-005-5 R2
	Service ACL filter	CIP-003-6 R2 CIP-005-5 R1 CIP-007-6 R1/R3
	NGE	CIP-003-6 R2 CIP-005-5 R2
	IPSec	CIP-005-5 R2
	Stateful zone-based firewall	CIP-005-5 R1 CIP-007-6 R1/R3
	VPRN routing table size limit and alarm notification	CIP-007-6 R1
	VPLS MAC table size limit and alarm notification	

7705 SAR Security Features	7705 SAR Implemented Functionalities	Applicability to CIP Requirements
User authentication	Local	CIP-007-6 R5
	RADIUS	
	TACACS+	
	Password management	
User authorization	Local	CIP-007-6 R5
	RADIUS	
	TACACS+	
Network access filter	Network ACL filter	CIP-005-5 R1 CIP-007-6 R1/R3
User accounting	RADIUS	CIP-007-5 R4 CIP-011-1
	TACACS+	
Event logging	Security log	CIP-005-5 R1 CIP-007-6 R4
	Change log	CIP-005-5 R1 CIP-010-1 R2
Configuration and management security	Configuration authorization	CIP-007-5 R5
	Configuration change logging	
	Security logging	
	Configuration backup	
	SNMPv3	CIP-005-5 R2
	SSH1/SSH2	
	SCP	
	Login control and exponential back-off	CIP-005-5 R2 CIP-007-6 R5
	Login banner customization	
	Session idle time-out	

7705 SAR Security Features	7705 SAR Implemented Functionalities	Applicability to CIP Requirements
Physical security	Ports closed by default	CIP-007-6 R1
	802.1x	CIP-007-6 R1
	Facility alarm integration	CIP-003-6 R2 CIP-006-5 R1
	CPM filter and CPM traffic management	Not required. But can provide extra reliability.
	Dedicated management routing instance	
	Non-Stop Routing (NSR)	
	Non-Stop Forwarding (NSF)	
	Non-Stop Signaling (NSS)	
	Graceful Restart (Helper)	
	Equal Cost Multi-Path (ECMP)	
	Fast Re-route (FRR)	
	Bidirectional Forwarding Detection (BFD)	
Control plane security	MD5 Authentication (OSPF, RSVP-TE, BGP4, IS-IS, RIP and LDP)	CIP-005-5 R1
	BGP4 AS path filtering	
	BGP4 prefix limiting	
	Generalized TTL Security Mechanism	
	(GTSM)/RFC 5082	

For further information on the complete Nokia IP/MPLS and NMS offering in relation to NERC CIPv5, please refer to the Nokia Mission-Critical Communications Network Solutions for Power Utilities, Attaining NERC CIP Version 5 Reliability Standards Compliance [2] application note.

Conclusion

This document provides an overview of the 7705 SAR's security capability. These capabilities should be applied within a standardized security framework. The ITU-T X.805 Security Architecture in general, and NERC CIPv5 in particular, have provided systematic frameworks that allow the feature functionality of the 7705 SAR to be reviewed within the end-to-end network. The features available on the platforms address potential threats on the data plane, control plane and management plane to infrastructure and services.

Nokia has real-world expertise in converged scalable network service delivery, resilient high availability and field-proven cyber security best practices. Our industry-leading mission-critical communications networks solution not only delivers the required network reliability, performance and scalability, it also serves as a bulwark defending against security threats and intrusions. Nokia can contribute significantly to your efforts to protect the grid and comply with regulatory requirements.

NOKIA

Acronyms

3DES	Triple DES
7705 SAR	Nokia 7705 Service Aggregation Router
AAA	authentication, accounting and authorization
ABR	area border router
ACL	access control list
AES	Advanced Encryption Standard
AES-128	AES with 128-bit key size
AES-256	AES with 256-bit key size
ALG	application level gateway
AS	autonomous system
ASBR	autonomous system border router
BES	Bulk Electricity System
BFD	bidirectional forwarding detection
BGP4	Border Gateway Protocol version 4
Cpipe	circuit pipe
CIP	critical infrastructure protection
CLI	command line interface
CPM	Control Processor Module
DAN	distribution automation network
(D)DoS	(distributed) denial of service
DES	Data Encryption Standard
DNAT	destination NAT
DNS	domain name system
DoS	distributed denial of service
DSCP	DiffServ Control Point
Epipe	Ethernet VLL
ECMP	Equal-cost multi-path
ESP	Encapsulating security payload
FAN	field area network
FERC	Federal Energy Regulatory Commission

FRR	Fast Re-route
GRT	global routing table
HMAC	Hash-based message authentication code
Ipipe	IP interworking VLL service
ICMP	Internet Control Message Protocol
ICV	integrity check value
IDS	intrusion detection system
IEC	International Electrotechnical Commission
IES	Internet enhanced service
IKE	Internet key exchange
IPS	intrusion prevention system
IPSec	IP Security (protocol suite)
IS-IS	Intermediate System-to-Intermediate System
ITU-T	International Telecommunication Union – Standardization Sector
LDP	Label Distribution Protocol
LSP	label switched path
MAC	Media Access Control
MD5	Message Digest 5
MP-BGP4	Multiprotocol BGP4
MPLS	Multiprotocol Label Switching
NAPT	network address port translation
NAT	network address translation
NERC	North American Electric Reliability Corporation
NSF	Non-Stop Forwarding
NSR	Non-Stop Routing
NSS	Non-Stop Signaling
OAM&P	operations, administration, maintenance and provisioning
OSPF	Open Shortest Path First
PPP	Point-to-Point Protocol
RADIUS	Remote Authentication Dial-In User Service
RIPv2	Routing Information Protocol version 2

RRI	reverse route injection
RSVP-TE	Resource Reservation Protocol – Traffic Engineering
SAP	service access point
SCADA	Supervisory Data Control and Acquisition
SCP	Secure Copy
SHA	Secret hash algorithm
SNAT	source NAT
SNMPv3	Simple Network Management Protocol version 3
SPI	Security Parameter Index
SSH	Secure Shell
TACACS+	Terminal Access Concentrator Access Control Server Plus
TDM	Time Division Multiplexing
TTL	Time to live
UDP	User Datagram Protocol
VLAN	virtual LAN
VLL	Virtual Leased Line
VMS	video management system
VPLS	virtual private LAN service
VPN	virtual private network
VPRN	virtual private routed network

References

1. Nokia. “Seamless Encryption for Mission-Critical Networks” http://resources.Nokia.com/sset/187584
2. Nokia. “Nokia Mission-Critical Communications Network Solutions for Power Utilities, Attaining NERC CIP Version 5 Reliability Standards Compliance.” MKT2014107732EN_Attaining_NERC_CIP_Compliance_AppNote.pdf
3. Congressional Research Service. “Electric Utility Infrastructure Vulnerabilities: Transformers, Towers, and Terrorism,” April 9, 2014. https://www.fas.org/sgp/crs/homesec/R42795.pdf
4. Federal Energy Regulatory Commission, Washington, DC, USA. RM13-5-000, Version 5 Critical Infrastructure Protection Reliability Standards, Nov. 22, 2013. http://www.ferc.gov/whats-new/comm-meet/2013/112113/E-2.pdf
5. IETF. RFC 793 Transmission Control Protocol https://datatracker.ietf.org/doc/rfc793/

6. International Electrotechnical Commission. IEC 62351, Power systems management and associated information exchange - Data and communications security, Part 1 to Part 8. http://www.iec.ch/smartgrid/standards/
7. International Telecommunication Union - Telecommunication Standardization Sector. ITU-T X.805, Security architecture for systems providing end-to-end communications, October 2010. http://www.itu.int/rec/T-REC-X.805-200310-I/en
8. Reilly, Steve. USA Today. March 24, 2015. “Bracing for a big power grid attack: ‘One is too many.” http://www.usatoday.com/story/news/2015/03/24/power-grid-physical-and-cyber-attacks-concern-security-experts/24892471/

Nokia is a registered trademark of Nokia Corporation. Other product and company names mentioned herein may be trademarks or trade names of their respective owners.

Nokia Oyj
Karaportti 3
FI-02610 Espoo
Finland
Tel. +358 (0) 10 44 88 000

Product code: PR1511016048EN