Juniper SRX Technologies

Course Introduction

ine.com

Piotr Kaluzny

CCIE #25665

pkaluzny@ine.com
linkedin.com/in/piotrkaluzny

CCIE Security

Course Prerequisites

+ Network security principles
+ SRX CLI basics

Course Objectives

- Describe Application Firewall & configuration process
- Describe User Firewall & authentication types
- Describe IDP concepts & components
- Define UTM & describe its components
- Understand VPN tunnel establishment
- Implement Site-Site VPN

Juniper SRX Technologies

Application Firewall

ine.com

Module Overview

- Introduction
- Application Identification
- Application Firewall flavors

Introduction to Application Firewall

- Traditional stateful firewalls use L3/L4 data for their policy decisions
  - E.g. DNS -> TCP/UDP port 53, HTTP -> TCP port 80
- Today's applications can easily fool the old-style detection engines
  - Custom (arbitrary) port numbers
  - HTTP/HTTPS tunneling
- Application Firewall (AppFW) enables L7 policy enforcement
  - Based on application signatures rather than ports
    - E.g. able to tell the difference between Facebook & Twitter
  - Requires Application Identification license & app signature package

Application Identification

- Application Identification (AppID) recognizes traffic based on several elements
  - Application signatures
  - Protocol parsing & decoding
  - Session management

- Main Features
  - Micro-applications & services detection
    - E.g. chat vs file transfer vs login
  - Encrypted traffic support
  - Unknown application (Junos:UNKNOWN)

AppFW Flavors

- AppFW comes in two flavors
  - Traditional
    - Before Junos OS 18.2
  - Unified Policies
    - Junos OS 18.2 and above

Traditional AppFW

- Refers to a dedicated AppSecure services module
  - The traffic of interest must be first "redirected" for additional inspection

- Traffic processing
  - Security Policy
    - Context
    - Traffic classification
    - Policy "permit" action
      - **permit application-services application-firewall rule-set** *ruleset_name*
  - Services Module
    - Application classification

Traditional AppFW

- Rule Set Example

```
rule-sets AFW_RSET {
    rule r1 {
        match {
            dynamic-application junos:FACEBOOK-CHAT;
        }
        then {
            reject { block-message; }
        }
    }
rule r2 {
    match {
        dynamic-application-group junos:gaming;
    }
    then { deny; }
```

Unified Policies AppFW

- Enforces L7 policies directly from the Security Policy
  - Another set of "match" conditions
- Unified Policies Example

```
security dynamic-application profile PROF redirect-message type custom-text content "THIS APP IS BLOCKED"

security policies from-zone trust to-zone untrust policy P1 match source-address any
security policies from-zone trust to-zone untrust policy P1 match destination-address any
security policies from-zone trust to-zone untrust policy P1 match application any
security policies from-zone trust to-zone untrust policy P1 match dynamic-application junos:YAHOO-MAIL

security policies from-zone trust to-zone untrust policy P1 then reject profile PROF
```

Juniper SRX Technologies

User-based Firewall

ine.com

Module Overview

- Introduction
- Authentication types, methods & operations

Introduction to User-based Firewall

- IP-based policies are no longer sufficient
  - Single user, multiple devices
  - Visibility
  - Logging & more
- User authentication can identify users & enable identity-based access
  - Granular per-user and/or per-group Security Policy rules
    - Teams, departments, guests, etc.
  - Improves visibility, logging, reporting & forensics

Authentication Types

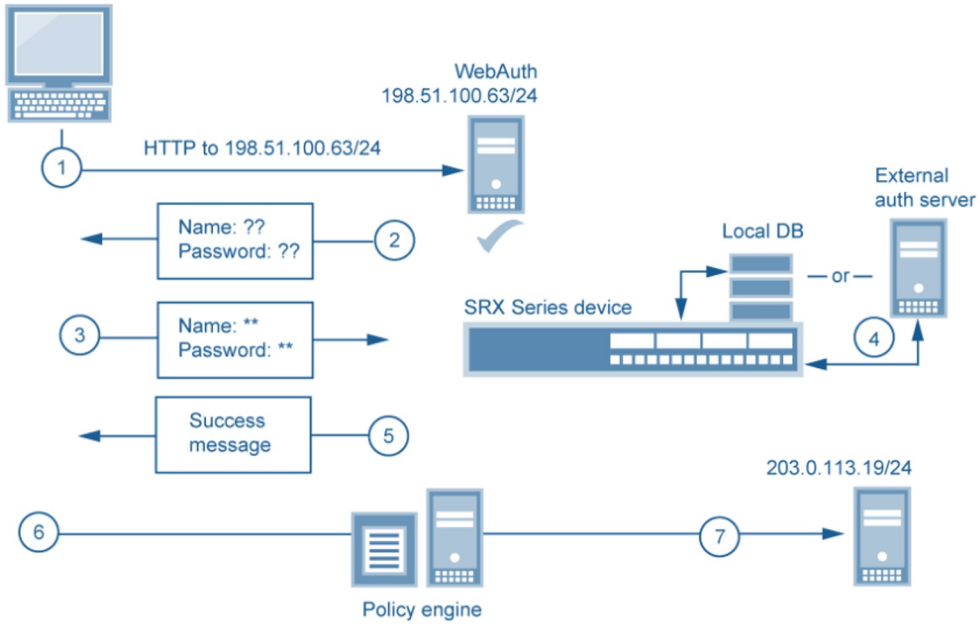
- User authentication can be enabled with one of two methods
  - Web Authentication
    - Requires authentication to the SRX prior to sending traffic
      - HTTP[S] based
  - Pass-Through
    - Authentication is triggered transparently
      - SRX buffers the first data packet & prompts for authentication
    - Supported for FTP, Telnet or HTTP[S]
    - Web redirection provides a seamless authentication experience
      - No need to reconnect after authentication
      - Applies to HTTP[S] only

Authentication Considerations

- Authentication Methods
  - Local
  - RADIUS
  - LDAP/AD
    - Supports Integrated User Firewall
  - SecurID

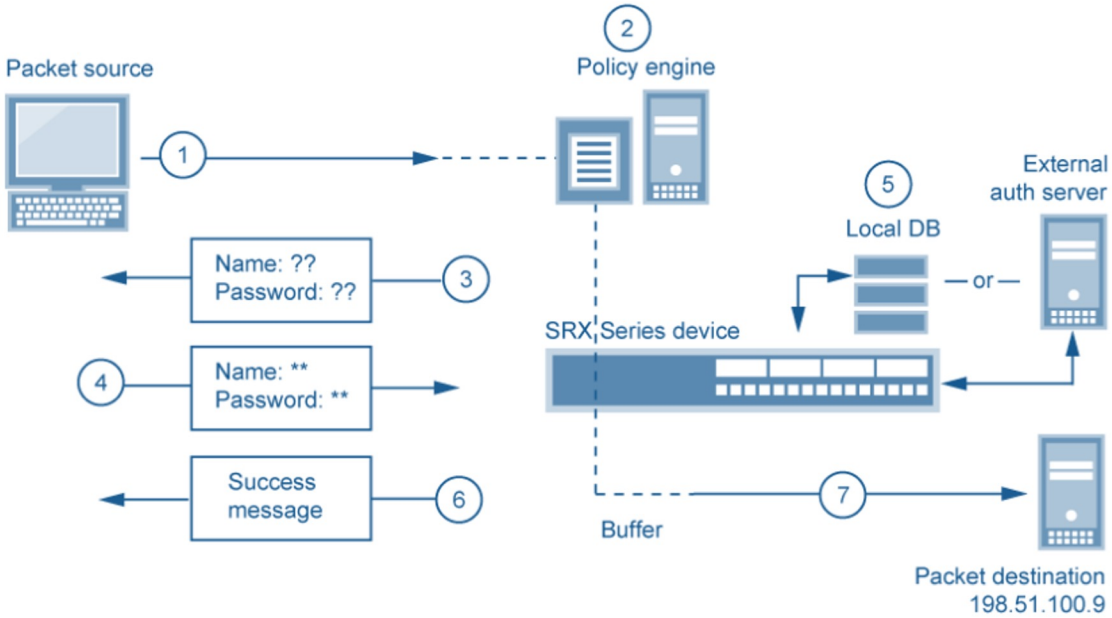
- Configuration Overview
  - Security Policy
    - Requires a rule that matches traffic to trigger authentication
      - permit firewall-authentication [pass-through | web-authentication]
  - External Database

Web-Authentication - Operations



source: juniper.net

Pass-Through Authentication - Operations



source: juniper.net

Juniper SRX Technologies

Intrusion Detection and Prevention Concepts

ine.com

Module Overview

+ IDP overview
+ IDP components

Intrusion Detection & Prevention Overview

- Stateful & application firewalling don't do much to stop attacks
  - Permitted traffic is not security-monitored
- Intrusion Detection & Prevention (IDP)
  - Scrutinizes traffic at bit-level to determine context & patterns
    - Detects (and stops) known (and possibly unknown) attacks
    - Resource-intensive
  - Integrated to Junos OS under the standard license
    - A special license is needed to keep the IDP databases up to date

IDP Signatures

- A signature is a set of predefined rules looking for known attack patterns
  - Groups of signatures are packaged and stored in a local database
- Signature Database
  - Detector Engine
    - Protocol decoder
  - Attack Database
    - Attack definitions
  - Application Signature Database
    - Application definitions
- The signature database should be always kept up to date

IDP Policy

- IDP enforcement is controlled through a policy
  - Determines what traffic to inspect
  - Made up of Rulebases

- Enabling IDP
  - Security Policy
    - **permit application-services** *idp-policy-name*

IDP Rulebases

- IDP uses a concept of Rulebases
  - An ordered set of rules that use a specific detection method
  - Rulebase types
    - Exempt
      - Used to exclude known false positives
      - Used to exclude certain sources and/or destinations
    - IPS

IDP Rules

- Instructions for the detection mechanisms
  - Match conditions
    - Zones
    - IP addresses
    - Application
  - Attack objects & groups
  - Action
  - Notification
    - Logging

IDP Rules

- Attack Objects
  - Known attack patterns
    - Signature
    - Protocol Anomaly
    - Compound
- Actions
  - No action
  - Ignore connection
  - Drop packet/connection
  - Diffserv Marking
  - IP actions

Juniper SRX Technologies

Advanced Threat Prevention Concepts

ine.com

Module Overview

- Advanced Threat Prevention overview
- ATP operations
- ATP Cloud integration

Advanced Threat Prevention (ATP) Overview

- Security framework for evolving threat/malware protection
  - Able to uncover & stop zero-day malware
  - Uses advanced detection methods
    - Machine learning, advanced file analysis & more

- ATP Deployments
  - Cloud-based (ATP Cloud)
    - Public cloud management
    - SRX
  - On-premise
    - Physical (JATP400 & JATP700)
    - Virtual

Advanced Threat Prevention (ATP) Overview

- ATP Features
  - Malware Analysis
  - Encrypted Traffic Insight
    - Basic SSL/TLS visibility
  - SecIntel
    - Threat feeds
      - Domains, URLs, IP addresses
    - Adaptive Threat Profiling
      - Automatic custom threat feeds
  - Prevention & Mitigation
    - Blocking
    - NAC integration

ATP Operations

- Data Collection
  - Juniper ATP Appliance collector
  - SRX
- Data Extraction
  - Objects & files
- File Inspection
  - Extracted object/file is sent for inspection

ATP Operations

- Malware Analysis
  - Cache Lookup
    - Hash - Verdict
  - Antivirus Scan
    - Detects "familiar" threats
  - Static Analysis
    - Metadata, instruction types, entropy
  - Dynamic Analysis
    - Sandboxing

- As a result of analysis a final verdict number (0-10) is returned
  - A threat can be blocked by the Security Policy

ATP Cloud Integration

- Licensing
  - Free license has a very limited feature set
- Cloud Portal Registration
  - https://amer.sky.junipersecurity.net
  - https://euapac.sky.junipersecurity.net
  - https://apac.sky.junipersecurity.net
  - https://canada.sky.junipersecurity.net
- Device Enrollment
  - Only enrolled devices can send files for inspection
  - https://www.juniper.net/documentation/us/en/software/sky-atp/sky-atp/topics/task/sky-atp-download.html

Juniper SRX Technologies

Unified Threat Management Overview

ine.com

Module Overview

- What is Unified Threat Management?
- UTM Engines

What is Unified Threat Management?

- Unified Threat Management (UTM) consolidates several security features to protect the network against certain threats
  - Malware, SPAM, fake attachments & more
- UTM Features
  - Antivirus scanning
  - Antispam protection
  - Content filtering
  - Web filtering
- Licensing
  - https://www.juniper.net/documentation/en_US/junos/topics/topic-map/security-utm-licensing.html

Antivirus Scanning

- Inspects traffic & content against viruses & other malware
  - Made of a virus pattern database & scan engine
    - The pattern database should be kept up-to-date

- SRX uses two scanning engines
  - Avira
    - On-device scanning
  - Sophos
    - Cloud-based scanning
      - No need to download & maintain the database on the SRX
      - Local caching improves performance

Antispam Protection

- Inspects e-mail traffic to identify spam
  - Local lists (allow & block), open relays, proxy servers, zombies, known spam sources & more
- Spam can be blocked or tagged
  - Blocking
    - Connection
    - E-mail data
  - Tagging
    - Subject
    - Header

Content Filtering

- Controls web/email/FTP traffic based on identified content patterns
  - E.g. files, images or certain text strings
  - Often used to provide basic data loss prevention
- Content filtering operations changed in Junos OS 21.4R1
  - Content evaluation is done based on the object's content
    - MIME type, file extension or protocol command is ignored

Web Filtering

- Controls web traffic at the URL level
  - URLs or URL categories
- Web Filtering Solutions
  - Local
    - Allow & block lists
  - Redirect
    - External server (Websense)
  - Enhanced
    - Websense ThreatSeeker Cloud (TSC)
      - Categories (151+)
      - Reputation score

Juniper SRX Technologies

Virtual Private Networks & IPsec

ine.com

Module Overview

- What is VPN?
- IPsec overview, components & operations

Virtual Private Network (VPN) Overview

- Virtual Private Network (VPN) serves as a logical connection
  - Its primary function is to provide end-to-end connectivity
    - Usually built over an unsecured network, such as the Internet
- VPNs rely on Tunneling
  - A process of encapsulating the original packet into a new header
  - Relies on three protocols :
    - Carrier, Encapsulating & Passenger
- Not all VPN implementations are secure

IP Security (IPsec) Overview

- The most common implementation of VPNs
  - RFC 4301 „Security Architecture for the Internet Protocol”
  - Layer 3
- IPsec Security Services
  - Authentication
  - Data Confidentiality
  - Data Integrity
  - Anti-replay

IPsec Components

- IPsec consists of multiple protocols & standards
  - Internet Security Association & Key Management Protocol (ISAKMP)
    - A framework describing core IPsec functions for secure communication (RFC 2408)
      - Specifies that keying & authentication should occur
      - Describes the procedures to establish, negotiate, modify & delete tunnel information
  - Internet Key Exchange (IKE) is an implementation of ISAKMP
    - Performs main Control Plane functions, like key exchange, authentication, etc.
    - IKEv1 (RFC 2409) & IKEv2 (RFC 7296)

IPsec Components

- IPsec heavily relies on Cryptography
  - Control Plane
    - Key Management : DH, ECDH
    - Authentication : PSK, RSA, ECDSA
  - Data Plane
    - Security Protocols : ESP, AH
    - Confidentiality : DES, 3DES, AES, SEAL
    - Data Integrity and Origin Authentication : MD5, SHA-1, SHA-2
- IPsec is a framework of open standards
  - Obsolete technologies can be replaced without changing the framework

IPsec Operations

- Negotiation Goals
  - Policy agreement
  - Key establishment
  - Authentication
  - Data protection
  - Maintenance

- IPsec VPNs are negotiated (UDP 500/4500) in phases
  - Management/Control Connection
    - IKEv1 "Phase I" or IKEv2 "IKE_SA_INIT"
  - Data Channels
    - IKEv1 "Phase II" or IKEv2 "IKE_AUTH"

Juniper SRX Technologies

Implementing Site-to-Site VPN

ine.com

Module Overview

- Implementation methods
- Configuration syntax
- Example

Implementation Methods

- SRX allows for two VPN implementations
  - Policy-based & Route-based
    - https://www.juniper.net/documentation/us/en/software/junos/vpn-ipsec/topics/task/security-comparison-policy-based-vpn-route-based-vpn.html

Route-Based Configuration

- VPN Interface & Routing
  - Tunnel Interface
    - **interfaces** *st_if_name* **unit family**
      - Zone assignment
      - Allowed services
        - **host-inbound-traffic system-services ike**
  - VPN Routes
    - **routing-options static route** *prefix* **next-hop** *st_if_name*

Route-Based Configuration

- IKE
  - Proposal
    - **security ike proposal**
      - Authentication method, encryption, integrity, DH
  - Policy
    - **security ike policy**
      - Proposal, mode, authentication key
  - Gateway
    - **security ike gateway**
      - Policy, peer address, interface

Route-Based Configuration

- IPsec
  - Proposal
    - **security ipsec proposal**
      - Protocol, encryption, integrity
  - Policy
    - **security ipsec policy**
      - Proposal
  - VPN
    - **security ipsec vpn**
      - Tunnel interface
      - IKE gateway
      - IPsec policy
      - Proxy identities & tunnel establishment

Route-Based Configuration

- Security Policy
  - Permit VPN traffic
- Verification
  - IKE
    - show security ike security-associations [detail]
  - IPsec
    - show security ipsec security-associations [detail]
    - show security ipsec statistics

Juniper SRX Technologies

ine.com

Course Conclusion

- Traditional firewalls can be easily fooled by modern applications
- User authentication enables identity-based (rather than IP-based) access
- Firewalls can block traffic but not necessarily network attacks
- SRX offers advanced malware protection through UTM
- VPNs provide secure connectivity for users & remote locations

Thank You