EXECUTIVE SUMMARY

Large-Scale security posture change from “Permit All” to “Deny All” with a transition from **Juniper SRX firewalls to Palo Alto firewalls**. Analyze over 100,000 daily traffic flows using PAN Expedition for the creation of new specific userID, appID rulesets.

STATEMENT OF WORK – Juniper SRX to Palo Alto 5280

Project Objectives:

a. Transition and cutover current ‘core’ firewall zone on two (2) pairs of Juniper SRX to (1) one pair of Palo Alto 5280 firewalls and one (1) pair of Palo Alto 5220.
b. Using Palo Alto’s Expedition analyze current core traffic and implement a ‘deny all’ posture with specific AppID+UserID allow/permit rules to allowed traffic through the Palo Alto firewalls.
c. Convert Juniper configurations to Palo Alto configurations and implement newly devised rulesets
d. Provide 15-day business continuity post-cutover support until steady state is achieved

II. Expedition Installation
a. Installation of Palo Alto firewall and Expedition
b. Perform network discovery and analysis to determine the optimal placement of the Palo Alto firewall within ABank’s network for the purpose of analyzing current CORE traffic on the "CORE" zones.
c. Configure Palo Alto firewall on ABank’s network to receive traffic for analysis.
i. Configure **Gigamon** to send/mirror 'clean' CORE traffic to logging server for analysis.
ii. Install Expedition Migration Tool on the ABank server
1. https://live.paloaltonetworks.com/t5/Expedition-Migration-Tool/ct-p/migration_tool
a. minimum requirements:
i. 4 CPUs
ii. 16GB RAM
iii. 100GB Disk Space
iv. Verify one (1) Palo Alto firewall has network access to Expedition
iii. Configure PAN firewalls to export logs to Expedition server
iv. Configure Expedition to ingest traffic logs.

III. Rule Discovery and Refinement
i. Refine existing legacy packet filter Security Policies for one (1) Juniper SRX firewall pair:
1. Configure daily log exports on one (1) Palo Alto firewall to the verified working Expedition server
ii. Perform iterative analysis of exported firewall logs to produce security policy rules
iii. Create net new security policies based on manual effort, log ingestion, and Expedition machine learning
iv. Analyze CORE traffic logs and patterns for the purpose of creating new rules to permit legitimate CORE traffic through the firewall.
v. Present and review the current CORE traffic logs to ABank personnel to determine legitimate vs. illegitimate traffic.
vi. Create a draft of new security rulesets--Layer 7 rulesets will be priority with L3/4 rulesets being used as necessary.

For more info, contact:
FireOwls Corporation – All-CCIE Team
16755 Von Karman Ave, #200, Irvine, CA 92602
info@fireowls.com | 1(833) Fire-Owl

vii. Review net new security policies with ABank to determine if rules are approved for configuration and commit operation
viii. Plan and prepare implementation of net new security policies and refined security policies

IV. Best Practices Configuration and Staging
  a. Pre-Cutover Preparation
    i. Draft notification emails for distribution to the appropriate stakeholders
    ii. Draft change request(s) for implementation and rollback
    iii. Engage and schedule stakeholders to perform validation testing
    iv. Schedule Internet service provider technician to clear ARP if circuit(s) terminated on layer-2 device
  b. Stage & Configure (1) HA Pair of (2) two PAN Firewalls.
    i. Onsite - Stage new PAN firewalls for integration into the ABank network
    ii. Onsite - Configure management interface and routing functionality (if necessary) to receive CORE traffic
    iii. Perform PAN-OS upgrade, dynamic updates, licensing updates and content database update
    iv. Configure PAN IDS/IPS, Threat Prevention and Wildfire to default best practice posture (tuning is not included)
    v. Configure new rule sets between CORE and ABank zones on new PA-5280 HA pair at Zayo data center and existing PA-5220 HA pair at ABank data center.
    vi. PAN firewall policies to be configured and pushed from existing ABank Palo Alto Networks Panorama.

V. Cutover - Onsite
  a. Onsite - Cutover CORE traffic from the Juniper SRX onto PAN firewalls.
  b. Re-confirm LAN and WAN configurations and proper traffic flow before deny-rule commit.
    i. Monitor matches/Core/denies on rulesets
    ii. Confirm Wildfire and Threat Defense is functional
    iii. Implement deny-any-rule posture.
    iv. Perform validation testing with stakeholders
    v. Perform HA validation testing
    vi. Perform failover test
    vii. Perform validation testing during failover

VI. Cutover Production Traffic – Two (2) Palo Alto firewalls as one (1) High Availability (HA) pair in active/standby:
  a. Export Staged Palo Alto firewall policy configuration to HA pair
  b. Perform PAN-OS upgrade, dynamic updates, licensing updates and content database updates
  c. Perform Palo Alto current best practices configuration
  d. A checklist will be sent to CLIENT for approval as some of these best practices may exceed CLIENT Information Security Policy (ISP) and audit requirement
  e. Perform cutover from SRX firewall to Palo Alto firewall:
    i. Cleary define success criteria with CLIENT and engage stakeholders to perform validation testing
    ii. Schedule Internet service provider technician to clear ARP if circuit(s) terminated on layer-2 device
    iii. Perform cutover
    iv. Perform HA validation testing

v. Perform failover test
vi. Perform validation testing during failover
vii. Complete implementation of net new security policies
viii. Provide post-implementation support up to change request success criteria acceptance and/or change request rollback plan completion

VII. Post-Cutover Support: FireOwls will provide post-cutover remote Support services, including emergency support, moves/adds/changes, and alerting (email/text) for 30 business days after cutover.

a. 30-day Business Continuity Support Services for the following platforms: Palo Alto Networks and Juniper SRX
b. Support schedule is Monday – Friday between 7am – 11pm Pacific
c. One lead Palo Alto expert will be assigned to service ABank for the purpose of network emergencies arising post-cutover due to the PAN firewalls.
d. One Client Services Manager will be assigned to ABank to engage FireOwls' extended CCIE team in case of network emergencies.
    i. Direct-dial telephone to lead PAN expert and Client Services Manager
    ii. Service requests of moves, adds, and changes
        1. MAC service SLA: 4 hours
    iii. Provide eight (8) hours of training for ABank staff
    iv. Provide network diagram of integration of the PAN firewalls into the ABank network
    v. Monitor steady state of firewall and provide a single weekly report of traffic pattern with rulesets: allows and denies.
    vi. Firewall monitoring and alerting - Automated Network Monitoring and Alerting of Networking Emergencies (if approved by Client, requires snmp/netflow configuration to offsite destination IP)
    vii. Alerting service is on for 30 days
    viii. Alerts will be sent to Client and FireOwls All-CCIE Team

For more info, contact:
FireOwls Corporation – All-CCIE Team
16755 Von Karman Ave, #200, Irvine, CA 92602
info@fireowls.com | 1(833) Fire-Owl